REMARKS

Double Patenting

The examiner provisionally rejected Claims 8-13, and 17-22 on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 5-10 of Application/Control Number: 10/701,154.

Applicant will consider timely submission of a terminal disclaimer in compliance with 37 CFR 1.321 (c) or 1.321 (d) to overcome the rejection upon indication of allowable subject matter.

The examiner rejected Claim 24 under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The examiner stated: "Claim 24 is a method "method of detecting a failed host" which results in an abstract idea. The claim limitations are merely steps of a computation or a formula. The limitations of "determining" and "indicating" describe a method where the result is an abstract idea." Applicant has amended claim 24 to claim the method in a computing device. The invention is concrete and tangible and thus the rejection has been overcome.

The examiner rejected Claim 24 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The examiner contends that: "[T]he limitations "greater than M" and "less than R" are not definite and it is not clear as to what the definitions of these limitations are according to the Specifications."

Applicant's specification clearly sets forth these limitations. For example, Applicant describes: A Host "A" becomes a "candidate" for a failed host analysis if both a mean profiled rate of server response packets from the Host "A" is greater than M 112, and the ratio of (standard deviation of profiled rate of server response packets from the host) to (mean profiled rate of server response packets from the host) is less than R 114." That is, the system 10

analyzes hosts that are uniformly "chatty", e.g., have relatively high volumes of traffic over regular periods. This analysis avoids false positives for quiet hosts, or hosts with long periods of inactivity. If these two factors are present then the host is flagged as a candidate failed host."

The exact values of M and R however are design criteria and are governed based on historical considerations, e.g., uniformly chatty and quite hosts. Therefore, this rejection is improper and should be removed.

The examiner rejected Claims 1-5 and 8-22 under 35 U.S.C. 102(e) as being anticipated by Malan et al. (U.S. PGPUB No. 20020032871).

Claim 1 is distinct over Malan et al. (Malan) since the reference fails to describe or suggest *inter alia* … a plurality of collector devices … to collect connection information to identify host connection pairs from packets that are sent between nodes on a network and an aggregator device … which produces a connection table that maps each node on the network to a record that stores information about traffic to or from the node. The examiner stated:

> **As per claim 1, Malan discloses a system, comprising:**
> **a plurality of collector devices that are disposed to collect statistical information on packets that are sent between nodes on a network (page 5, paragraph [0066]) and (Fig. 4, elements 20, 20b).**
> **an aggregator (page 5, paragraph [0071], lines 7-11) and (page 3, paragraphs [0032], [0033], and [0034]) that receives network data from the plurality of collector devices, and which produces a connection table that maps each node on the network to a record that stores information about traffic to or from the node (page 5, paragraphs [0066] and [0067]).**

Malan fails to disclose an aggregator device which produces a connection table, as claimed. Malan Fig. 5, element 20a is neither a connection table nor a store for a connection table that stores a record about traffic to or from the node. Element 20a is merely an input buffer that stores statistical data collected by the collector.

According to Malan, in paragraphs [0032] to [0034] what is collected is statistical information on packets seen by the collectors. In [0033] Malan teaches to aggregate according to one invariant feature, which Malan discloses in [0035] as source and destination endpoints. However, this fails to describe collector devices that provide the network data used by the aggregator.

The examiner further relies on Malan [0067] and [0068] to teach "a connection table that maps each node on the network to a record that stores information about traffic to or from the node." Malan [0067] and [0068] are reproduced below

> **[0067] The input buffer 20a, located on collector 20, is adapted to normalize or categorize the data packet flow statistical information and to generate a number of records including the normalized data packet flow statistical information. The storm detector 20b is adapted to detect the data packet flow anomalies by comparing the records to an anomaly pattern and/or a predetermined threshold. If components of the normalized data packet flow statistical information exceed the predetermined threshold, a data packet flow anomaly is detected. Thereafter, the detected data packet flow anomaly and data associated with the data packet flow anomaly, such as the source and destination addresses of the flow information can be stored in the detector database 20c.**
>
> **[0068] The storm profiler module 20d is adapted to receive the normalized data packet flow statistical information or records from the input buffer 20a and to generate the predetermined threshold, which is concomitantly communicated to the storm detector module 20b. In this configuration, the predetermined threshold defined in the storm detector is adaptively adjusted based on changing trends or profiles of the normalized data packet flow statistical information received by the storm profiler 20d. The changing trends or profiles of the normalized data packet flow statistical information, for example, can include changes in the average bandwidth allocated to each of the computer systems 16 during a particular period of time or changes to the number of computer systems 16 communicating information at the same instant of time.**

Thus, while Malan discloses that the collector is adapted to: "normalize or categorize the data packet flow statistical information and to generate a number of records including the normalized data packet flow statistical information." Malan [0068], Malan fails to disclose that the buffer stores a "connection table that maps each node of a network to a record object that stores information about traffic to or from the node," and hence fails to describe or suggest the claimed aggregator.

Rather, Malan [0064] describes what is meant by the data packet flow statistical information. According to Malan:

> **[0064] ... The packet flow statistical software running on each of the routing systems 22, 22b and 22c enable each of the routing systems 22, 22b and 22c to gather and store data packet flow statistical information. The data packet flow statistical information can include the number of packets which have been communicated between computer systems 16, the duration of communication between each of the computer systems 16, the total number of packets communicated over each LAN (which is typically used for capacity planning) as well as other various data packet flow statistical information.**

Malan also discloses processing of the data packet flow statistical information. According to Malan, in paragraph [0067] (reproduced in its entirety above), "The input buffer 20a, located on collector 20, is adapted to normalize or categorize the data packet flow statistical information and to generate a number of records including the normalized data packet flow statistical information." Malan thus discloses to generate statistical information not a connection table. Further Malan discloses: "The storm detector 20b is adapted to detect the data packet flow anomalies by comparing the records to an anomaly pattern and/or a predetermined threshold." Again, Malan discloses to compare records (containing the normalized statistical information) to an anomaly pattern and/or a threshold. Malan then tests to see "If components of the normalized data packet flow statistical information exceed the predetermined threshold," in order to detect a data packet flow anomaly.

Malan also discloses to thereafter, store "the detected data packet flow anomaly and data associated with the data packet flow anomaly, such as the source and destination addresses of the flow information … ." Thus, Malan while mentioning that: "data associated with the data packet flow anomaly, such as the source and destination addresses of the flow information can be stored in the detector database 20c," Malan fails to disclose the data is stored in a manner "that maps each node of a network to a record object that stores information about traffic to or from the node," as required by claim 1.

Thus, in no sense does Malan disclose or suggest that the collector or any other device in Malan builds a connection table, much less an aggregator that receives connection information from the plurality of collector devices and produces a connection table …, as generally recited in claim 1. Accordingly, claim 1 is neither described nor suggested by Malan.

Claim 2

Applicant amended claim 2 to more distinctly claim this feature of the invention. Claim 2, as originally presented, distinguished over Malan, at least for the reason that it depended from claim 1. However, as currently amended claim 2 now requires that … the aggregator determines at least in part from connection patterns derived from the connection table occurrences of network events.

The examiner contends that: "Malan discloses the aggregator determines occurrences of network events (page 5, paragraph [0071] and page 3, paragraph [0032])." While it may be true, that Malan determines network events, Applicant contends to the extent that Malan does so it is not at least in part from connection patterns derived from the connection table, but rather from the statistical data collected by the collectors. Accordingly, claim 2 serves to further distinguish over Malan.

Claim 3

Applicant has amended claim 3 to claim that … the aggregator further comprises a process that collect statistical information on packets that are sent between nodes on a network and which sends the statistical information to the aggregator. The examiner had rejected claim 3, which previously recited "communicates occurrences of network events to an operator." Claim 3 has been amended to recite a different feature and in particular recite an analogous feature as that disclosed by Malan, namely, collection of statistical information on packet flows. Claim 3 however distinguishes over Malan since Malan neither describes nor suggests that that aggregator receives the statistical information and the connection information as required by claim 3.

Claims 8-13

Each of these claims serves to further distinguish over Malan. The examiner stated:

> **As per claim 8, Malan discloses the connection table includes a plurality of records that are indexed by source address (page 5, paragraph [0067], lines 10-14).**
>
> **As per claim 9, Malan discloses the connection table includes a plurality of records that are indexed by destination address (page 5, paragraph [0067], lines 10-14).**
>
> **As per claim 10, Malan discloses the connection table includes a plurality of records that are indexed by time (page 5, paragraph [0067], lines 10-14).**
>
> **As per claim 11, Malan discloses the connection table includes a plurality of records that are indexed by source address, destination address and time (page 5, paragraph [0067], lines 10-14).**

Claims 8-13 serve to further distinguish over Malan. In rejection of claims 5-11, the examiner relies on: " indexed by source address (page 5, paragraph [0067], lines 10-14) … indexed by destination address (page 5, paragraph [0067], lines 10-14) … indexed by time (page

5, paragraph [0067], lines 10-14) … indexed by source address, destination address and time (page 5, paragraph [0067], lines 10-14)." Page 5, paragraph [0067], lines 10-14 from Malan are reproduced below:

> **[0067] … Thereafter, the detected data packet flow anomaly and data associated with the data packet flow anomaly, such as the source and destination addresses of the flow information can be stored in the detector database 20c.**

Applicant contends that not only does Malan fail to disclose the aggregator including the connection table as in claim 1, but Malan also fails to disclose in [0067] or elsewhere that the connection table includes a plurality of records that are indexed by source address, destination address and/or time, as claimed in claims 8-11. Indeed in [0067] Malan discloses that the detected data packet flow anomaly and data associated with the anomaly are stored in the detector database 20c. However, Applicant's claims are directed to the connection table in memory. Moreover, Malan discloses that the source and destination addresses of the flow information stored in the detector database 20c, as the data. Malan says nothing about how the data in the detector database 20c is indexed and clearly in [0067] Malan does not suggest that it is indexed by source address, destination address and/or time, as claimed. Indeed time is not even mentioned in [0067].

Claim 12 serves to further limit claim 1 by reciting that the connection table includes a plurality of connection sub-tables to track data at different time scales. The examiner contends that: "Malan discloses the connection table includes a plurality of connection sub-tables to track data at different time scales (page 5, paragraph [0074])." Paragraph [0074] is reproduced below:

> **[0074] More precisely, the correlator 24a is adapted to receive and categorize the alert messages and to generate a number of tables including the categorized alert messages. The tables including the categorized alert messages are stored in the alert message database 24b, which is coupled to the correlator module 24a. The correlator module 24a is further adapted to compare the alert messages to determine if trends exist. One example of a trend can be a plurality of alert messages that are traceable through the computer network system 10 to a particular computer system 16. Another example of trend can be a plurality of alert messages that include similar characteristics.**

Claim 12 is directed to the connection table and specifically a configuration of sub tables that track connections at different time scales. Malan [0074] discloses "categorize the alert messages and to generate a number of tables including the categorized alert messages." However, this teaching is neither relevant to the claimed connection table, which maps nodes of a network to record objects that store information about traffic to or from the node, nor to the claimed connection table including sub tables that track connections at different time scales.

Malan discloses that "to generate a number of tables including the categorized alert messages." According to Malan these are stored in the alert message database 24b, not database 20c which also contains the detected data packet flow anomaly and data associated with the data packet flow anomaly, such as the source and destination addresses of the flow information. Therefore, Malan does not suggest much less describe "the connection table and specifically a configuration of sub tables that track connections at different time scales," as claimed in claim 9.

Claim 13 further limits claim 12 by reciting that the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time. Malan, as discussed above, neither discloses nor suggests the connection table or connection sub-tables. Inherently, Malan fails to disclose a time-slice connection table … and at least one other sub-table that operates on a larger unit of time … Again, Malan [0074] is directed to alert messages not to a connection table.

Applicant's claim 14 is a method that includes analogous features as claim 1 and is allowable for reasons given in claim 1. Similarly claims 15-22 depend directly or indirectly form claim 14 and are allowable with claim 14 and for analogous reasons as given for certain of the dependent claims of claim 1, discussed above.

The examiner rejected Claim 23 under 35 U.S.C. 102(e) as being anticipated by Belissent (U.S. Patent No. 6,789,203). The examiner stated:

> **As per claim 23, Malan discloses a method of detecting a new host connecting to a network comprises:**

receiving statistics collected from a host in the network (page 5, paragraphs {0066} and {0067}).

Malan fails to explicitly disclose the relation of received packets over a period of time.

Belissent teaches:

and indicating to a console that the host is a new host if, during a period of time T, the host transmits at least N packets and receives at least N packets, and if the host had never transmitted and received more than N packets in any previous period of time with a duration of T (col. 4, lines 9-20 and col. 5, lines 62-67 through col. 6, lines 1-17). Belissent discloses a system for monitoring connection request rates over a period of time and a rejection threshold.

Applicant believes that the examiner intended to reject claim 23 as obvious over Malan in view of Belissent and will treat this rejection accordingly.

Indeed, Malan teaches receiving statistics collected from a host, namely the collector. However, applicant does not see Malan as teaching any technique for detection of new hosts. As for Belissent, Belissent teaches at (col. 4, lines 9-20) throttling the processing of new connections to thwart a denial of service attack, not the detection of new host connecting to a network. At (col. 5, lines 62-67 through col. 6, lines 1-17) Belissent teaches details of the throttling technique. However, neither the rejection rate R, nor the throttling interval n suggest indicating to a console that the host is a new host if, during a period of time T, the host transmits at least N packets and receives at least N packets, and if the host had never transmitted and received more than N packets in any previous period of time with a duration of T. The examiner argues that "Belissent discloses a system for monitoring connection request rates over a period of time and a rejection threshold." However, applicant is directed to packet transmission not specifically connection requests. It is not necessary for a host to make connection requests to the network in order to transmit over a network and thus be detectable as a new host, whereas, as in Belissent, in order to send packets to a server, gateway and the like connection requests are used.

The examiner rejected Claims 6 and 7 under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (U.S. PUB No. 20020032871) in view of Hill et al. (U.S. Patent No. 6,088,804).

Claim 6 is allowable over Malan and Hill at least for the reasons discussed in base claim 1.

As for claim 7, the examiner acknowledges that Malan et al. fails to explicitly disclose scanning attacks, unauthorized access and worm propagation, and relies on Hill to teach: "the anomalies include and scanning attacks (col. 4, lines 35-41) and "the anomalies include unauthorized access and worm propagation (col. 5, lines 57-65)."

Applicant contends that claim 7 is allowable for the reasons discussed in claim 1. In addition, while Hill mentions worms and the unauthorized actions, Hill does not address any specific teaching to detect those types of attacks in Hill's system. Moreover, Hill fails to cure the deficiencies in Malan. Accordingly, whether taken alone or in combination Malan and Hill fail to suggest claim 7.

The prior art cited but not applied is seen as neither describing nor suggesting applicant's invention, whether taken separately or in combination with the art of record.

Please charge the Petition for Extension of Time fee to Deposit Account no. 06-1050. Please apply any other charges or credits to Deposit Account no. 06-1050.

Respectfully submitted,

Date: 4/3/06

Dennis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906